IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: JEFFREY BRUCE LOTSPIECH ET AL.	)	
	)	Group Art Unit:
Serial No.: 10/691,361	)	2134
	)	
Filed: October 21, 2003	)	
	)	Examiner:
For: SYSTEM AND METHOD FOR SECURELY REMOVING CONTENT OR A DEVICE FROM A CONTENT-PROTECTED HOME NETWORK	)	Tran, Ellen C.

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

REAL PARTY IN INTEREST

The real party in interest is International Business Machines Corporation, the assignee of record as recorded at reel/frame 014644/0617.

RELATED APPEALS AND INTERFERENCES

There are no pending appeals or interferences related to this appeal.

STATUS OF CLAIMS

Claims 1, 4, 6-8, 11, 13-15, 98 and 99 stand finally rejected.

Claims 2-3, 5, 9-10, 12, 17-18 and 24-25 have been canceled.

Claims 16, 19-23, 26-97 have been withdrawn.

The rejections of claims 1, 4, 6-8, 11, 13-15, 98 and 99 are herein appealed.

STATUS OF AMENDMENTS

There have been no amendments filed after the final rejection mailed October 17, 2007.

SUMMARY OF CLAIMED SUBJECT MATTER

A concise explanation of the subject matter defined in each of the independent claims involved in the appeal is provided below.

Independent claim 1 recites a method for securely removing a device from at least one of a plurality of devices in a network while protecting a content from unauthorized use or distribution, the method comprising: calculating an encryption key for the protected content in the network, based at least in part on a list of the plurality of devices in the network (paragraph [0065]; Figure 3, step 305); tentatively marking the device for removal, by modifying the list of the plurality of devices in the network, wherein the list of the plurality of devices is included in an authorization table (paragraph [0065]; Figure 3, step 315); the device marked for removal automatically acknowledging the removal (paragraph [0066]; Figure 3, step 320); automatically recording the removal of the device in the authorization table (paragraph [0068]; Figure 3, step 325); recalculating the encryption key for all the devices remaining in the network and the protected content, using the modified list and the authorization table (paragraph [0069]; Figure 3, step 330) ; and reencrypting the protected content with the recalculated encryption key (paragraph [0069]; Figure 3, step 335).

Independent claim 8 recites a system for securely removing a device from at least one of a plurality of devices in a network while protecting a content from unauthorized use or distribution, the system comprising: an encryption key (Figure 2, element 206) that is calculated for the protected content in the network, based at least in part on a list of the plurality of devices in the network (paragraph [0065]; Figure 3, step 305); the device being tentatively marked for removal by modifying the list of the plurality of devices in the network, wherein the list of the plurality of devices is included in an authorization table (paragraph [0065]; Figure 3, step 315); the device marked for removal automatically acknowledging the removal (paragraph [0066]; Figure 3, step 320); the authorization table automatically recording the removal of the device (paragraph [0068]; Figure 3, step 325); the encryption key being recalculated for all the devices remaining in the network and the

protected content, using the modified list and the authorization table (paragraph [0069]; Figure 3, step 330); and the protected content being reencrypted with the recalculated encryption key (paragraph [0069]; Figure 3, step 335).

The above exemplary embodiments are discussed with respect to the aforementioned independent claims by way of example only and are not intended to in any way limit the scope of these claims.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 4, 6-8, 11, 13-15, 98 and 99 were rejected under 35 U.S.C. § 103 as being unpatentable over IBM Oct. 2001 (IBM Response to DVB-CPT Call for Proposals for Content & Copy Management: xCPCluster Protocol) in view of Xu.

ARGUMENT

Prior to discussing the rejections in detail, a summary of exemplary embodiments is provided. Embodiments of the invention provide for protecting content on a network from unauthorized use when a device is removed from a network. When a device is removed from a network, it acknowledges removal and a list of devices in the network is altered. Further, an encryption key for network devices is recalculated based on the modified list. Figure 3 illustrates a method for removing a device form a network and paragraphs [0065] – [0072] describe the method. This method prevents users from removing content from a network in an unauthorized manner.

Rejection of claims 1, 4, 6-8, 11 and 13-15

Claims 1, 4, 6-8, 11, 13-15, were rejected under 35 U.S.C. § 103 as being unpatentable over IBM Oct. 2001 (IBM Response to DVB-CPT Call for Proposals for Content & Copy Management: xCPCluster Protocol) in view of Xu. This rejection is traversed for the following reasons.

Claim 1 recites, *inter alia,* "recalculating the encryption key for all the devices remaining in the network and the protected content, using the modified list; and the authorization table." Neither IBM Oct. 2001 nor Xu teaches or suggests this feature. In applying the references the Examiner cites to IBM Oct. 2001 as allegedly teaching this

feature. The Examiner cites to page 7, paragraph 9 as teaching altering a binding key whenever a new device is introduced into the home. This is contrary to claim 1, which details a method of securely **removing** a device, not adding a device. The recalculating step in claim 1 is based on the modified list and the authorization table after a device is removed. A reading of the entire claim 1 reveals that the modified list is modified by a device being marked for removal and that the removal of the device is recorded in the authorization table. The recalculating of claim 1, when properly read in light of the entire claim, is not taught by IBM Oct. 2001 as IBM Oct. 2001 deals with adding a device to a network, not removal.

Further, IBM Oct. 2001 does not teach "recalculating the encryption key for all the devices remaining in the network and the protected content, **using the modified list; and the authorization table**." IBM Oct. 2001 makes reference to a media key, a network's binding ID and a network's authorization table. There is no teaching in IBM Oct. 2001 of using a list of devices in the network as part of the calculation of an encryption key. Xu also fails to teach this feature. In Xu the system updates a decryption key when a user terminates a multicast session (column 7, lines 13-17). Xu fails to teach recalculating a decryption key using a modified list and an authorization table. Thus, even if IBM Oct. 2001 and Xu are combined, these features of claim 1 cannot be taught.

The Examiner acknowledges that IBM Oct. 2001 fails to teach "tentatively marking the device for removal, by modifying the list of the plurality of devices in the network, wherein the list of the plurality of devices is included in an authorization table." The Examiner relies on Xu as allegedly teaching this feature. Applicants respectfully disagree. Xu broadly teaches updating a decryption key when a device terminates a session or at discrete intervals (column 7, lines 13-16). There is no reference that a device is marked for removal or that the device is being removed from the network. The device has terminated a session, not been removed from the network. Nor is there any teaching of modifying a list of devices that is included in an authorization table. The description of updating the decryption key discussed in Xu is sparse and simply does not include the features of claim 1. Thus, even if IBM Oct. 2001 and Xu are combined, the features of claim 1 do not result.

For at least the above reasons, claim 1 is patentable over IBM Oct. 2001 in view of Xu. Claims 4, 6, and 7 variously depend from claim 1 and are patentable over IBM Oct. 2001 in view of Xu for at least the reasons advanced with reference to claim 1.

Claim 8 recites features similar to those discussed above with reference to claim 1 and is patentable over IBM Oct. 2001 in view of Xu for at least the reasons advanced with reference to claim 1. Claims 11 and 13-15 depend from claim 8 and are considered patentable for at least the same reasons.

Rejection of claims 98 and 99

Claims 98 and 99 recite "calculating the encryption key includes calculating the encryption key in response to a management key from a key management block, a binding ID associated with each of the devices on the list and a hash of an authorization table listing authorized devices." It is important to note that claims 98 and 99 recite that the hash is on the authorization table, not on all the elements (i.e., management key, binding ID, and authorization table) used to compute the encryption key. In applying the references, the Examiner cites to page 7, paragraph 5 of IBM Oct. 2001. This section of IBM Oct. 2001 teaches computing a key based on a hash of three quantities: the media key, the network's binding ID and network's authorization table. Claims 98 and 99, however, only recite using the hash of the authorization table, not all three quantities. Thus, IBM Oct. 2001 does not teach the elements of claims 98 and 99. This is further exhibited by the Examiner's rejection, which cites only a portion of claim 98, and omits the language after the term "hash".

For at least the above reasons, claims 98 and 99 are patentable over IBM Oct. 2001 in view of Xu.

VII. Conclusion

In view of the foregoing, it is respectfully submitted that the application is in condition for allowance. Accordingly, it is respectfully requested that this application be allowed and a Notice of Allowance issued.

In the event the Commissioner of Patents and Trademarks deems additional fees to be due in connection with this application, Applicants' attorney hereby authorizes that such fee be charged to Deposit Account No. 09-0441.

Respectfully submitted,

By:_____

David A. Fox
Registration No. 38,807
CANTOR COLBURN LLP
55 Griffin Road South
Bloomfield, CT 06002
Telephone (860) 286-2929
Facsimile (860) 286-0115
Customer No. 67232

Date: March 14, 2008

CLAIM APPENDIX

1. A method for securely removing a device from at least one of a plurality of devices in a network while protecting a content from unauthorized use or distribution, the method comprising:

calculating an encryption key for the protected content in the network, based at least in part on a list of the plurality of devices in the network;

tentatively marking the device for removal, by modifying the list of the plurality of devices in the network, wherein the list of the plurality of devices is included in an authorization table;

the device marked for removal automatically acknowledging the removal;

automatically recording the removal of the device in the authorization table;

recalculating the encryption key for all the devices remaining in the network and the protected content, using the modified list; and the authorization table; and

reencrypting the protected content with the recalculated encryption key.

4. The method of claim 1, wherein recalculating the encryption key comprises including a key management block in the calculation.

6. The method of claim 1, wherein recalculating the encryption key comprises including the binding identification for the plurality of devices, excluding the device to be removed.

7. The method of claim 1, wherein the protected content is encrypted with a title key;

and further comprising reencrypting the title key with the recalculated encryption key.

8. A system for securely removing a device from at least one of a plurality of devices in a network while protecting a content from unauthorized use or distribution, the system comprising:

an encryption key that is calculated for the protected content in the network, based at least in part on a list of the plurality of devices in the network;

the device being tentatively marked for removal by modifying the list of the plurality of devices in the network, wherein the list of the plurality of devices is included in an authorization table;

the device marked for removal automatically acknowledging the removal;

the authorization table automatically recording the removal of the device;

the encryption key being recalculated for all the devices remaining in the network and the protected content, using the modified list and the authorization table; and

the protected content being reencrypted with the recalculated encryption key.

11. The system of claim 8, wherein the encryption key is recalculated using a key management block in the calculation.

13. The system of claim 8, wherein the encryption key is recalculated using the binding identification for the plurality of devices, excluding the device to be removed.

14. The system of claim 8, wherein the protected content is encrypted with a title key; and

further comprising the title key being reencrypted with the recalculated encryption key.

15. The system of claim 8, wherein the plurality of devices comprise any one or more of:

a television, a set top box, a personal video recorder, a video cassette recorder, a compact disk player, a compact disk player recorder, a personal computer, a portable music player, an audio player, a video player, a game console, and a personal network storage device.

98. The method of claim 1 wherein:

calculating the encryption key includes calculating the encryption key in response to a management key from a key management block, a binding ID associated with each of the devices on the list and a hash of an authorization table listing authorized devices.

99. The system of claim 8 wherein:

the calculated encryption key is calculated using a management key from a key management block, a binding ID associated with each of the devices on the list and a hash of an authorization table listing authorized devices.

EVIDENCE APPENDIX

Not Applicable

RELATED PROCEEDINGS APPENDIX

Not Applicable